REMARKS/ARGUMENTS

An interview was conducted with the Examiner Courtney D. Fields and the Examiner's supervisor on January 15, 2004 at 4:00 PM (EST). Based on the discussion during the interview, Applicants have amended independent claims 1, 9, and 17. The Examiner's supervisor indicated that if the amended independent claims are patentable over the prior art the claims would be entered.

Claim Rejections

The Examiner rejected pending claims 1-24 under 35 U.S.C. §102(b) as being unpatentable over Ault (US 6,338,064). Applicants have amended independent claims 1, 9, 17 and traverse the claim rejections.

Amended Independent Claims 1, 9, 17

Independent claims 1, 9, and 17 provide a method, system, and article of manufacture for accessing a control system in a server from a client computer, wherein the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations, further comprising:

requesting, with the client, a security context for the client including authorization to allow the client to access control system functions in the server, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context;

returning, with the server, the requested security context to the client; and

transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server.

Applicant has amended claims 1, 9, and 17 to include the limitations that the security context is associated with a client credential information including access for which the client is authorized and that the server is capable of impersonating the client to generate the security context. Support for the included limitations may be found in at least page 4, lines 20-23; page 6, line 28 - page 7, line 2; page 7, lines 11-13; page 11, lines 8-10; and pages 4-12 of the specification.

The Examiner has rejected the independent claims 1, 9, and 17 under 35 U.S.C. §102(b) as being unpatentable over Ault (Office Action Page 2). The cited Ault (col. 4, lines 27-35, 39-42, 45-48, 53-65) discusses accepting a client request at a server. The client request contains an authorization information that is analyzed by the server via a plug-in in the server. The server determines if the client can retrieve a document and if the client can retrieve the document then the server sends the document to the client.

The claims require requesting with the client a security context for the client, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context. The server returns the security context to client and the client uses the security context to access the server.

The cited Ault discusses that the client requests a document from the server, whereas the claims require that the client requests a security context. The document is a protected file in Ault (Ault: col. 1 lines 10-12), where Ault further describes that the server supports files in the form of hypertext documents and objects (Ault, col. 4: lines 9-10). Nowhere does the cited Ault teach or disclose the claim requirement that the client requests a security context, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context. The cited Ault discusses that the document that is requested by the Web browser (Ault: reference numeral 16) in the client (Ault: reference numeral 10) is a Web document, whereas the claims require the client to request a security context.

While the cited Ault does discuss impersonation of a client, the impersonation of the cited Ault is for obtaining a protected file for the client. The protected file discussed in Ault are Web documents (Ault: col 1: lines 9-12). The impersonation of the client discussed in Ault is for returning Web documents requested by the client, but the cited Ault does not teach or discuss the claim requirement of returning, with the server, the requested security context to the client. Therefore, not only is the Web document discussed in the cited Ault is different from the security context required by the claims, but the claim requirement of the server being capable of impersonating the client to generate the security context is neither taught nor disclosed by the cited Ault.

In the cited Ault, the client requests a Web document and the server impersonates the client to secure the Web document and return the Web document to the client. Even if for the sake of argument the Web document discussed in the cited Ault is interpreted to be the security context of the claim requirements (which the applicant disputes), nowhere does the cited Ault teach or disclose the claim requirement of transmitting with a client program executing in the client, the security context to access to the control system in the server. In contrast, the cited Ault discusses requesting the Web document from the client and receiving the Web document at the client.

Furthermore, nowhere does the cited Ault teach or disclose the claim requirement of the client requesting a security context, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context. Lines 53-65 of the cited Ault discusses a plug-in that facilitates users authentication so that uses of client machines may use browsers to access documents. However, Ault discusses that the plug-in is at the server (Ault: page 5: lines 37-42) and the plug-in is used for authentication. The user authentication discussed in the cited Ault is for returning a document and does not teach or disclose the claim requirement of returning, with the server, the requested security context to the client.

The Examiner found that col. 4, lines 27-35 of the cited Ault discloses the claim requirement of requesting with the client, security context for the client including authorization to allow the client to access control system functions in the server. Col. 4, lines 27-34 of the cited Ault discusses that the server accepts a client request and returns a response. Col. 4, lines 27-34 of the cited Ault further discusses that the operation of the server is governed by a number of functions executed in a certain sequence. The first function is the sequence is an authorization translation during which the server translates any authorization information sent by the client into a user and a group. Nowhere does the cited Ault (col. 4, lines 27-34) disclose the claim requirement of requesting with the client, security context for the client including authorization to allow the client to access control system functions in the server. In contrast, the cited Ault (col. 4, lines 27-34) discusses how the server performs a certain sequence of functions in the server on receiving a request form the client and not the requirement of requesting with the client, security context for the client including authorization to allow the client to access control system functions in the server as claimed. Authorizing the client's request as discussed in the cited Ault is for authorizing access to a document in the server, whereas the claims require requesting with the client, security context for the client including authorization to allow the client to access control system functions in the server.

The Examiner found that col. 4, lines 39-42 of the cited Ault discloses the claim requirement of returning with the server the requested security context to the client. Col. 4, lines 39-42 of the cited Ault discusses that the server performs various steps to determine if the client may retrieve a document. Nowhere does the cited Ault (col. 4, lines 39-42) disclose the claim requirement of returning with the server the requested security context to the client. In contrast, the cited Ault (col. 4, lines 39-42) discusses how the server determines whether a client may retrieve a document and not the requirement of returning with the server the requested security context to the client as claimed. The plug-in in the server discussed in col. 4, lines 53-65 of the cited Ault discusses a plug-in that facilitates user authentication so that users of client machines may use browsers to access documents. However, Ault discusses that the plug-in is at the server

(Ault: page 5: lines 37-42) and the plug-in is used for authentication. The plug-in in the cited Ault is for user authentication, whereas the claims require returning, with the server, the requested security context to the client.

The Examiner found that col. 4, lines 45-48 of the cited Ault discloses the claim requirement of transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server. Col. 4, lines 45-48 of the cited Ault discusses that the server selects an internal server function to send a result back to the client. Nowhere, does the cited Ault (col. 4, lines 45-48) disclose the claim requirement of transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server. In contrast, the cited Ault (col. 4, lines 45-48) discusses how the server sends a result back to the client. Nowhere does the cited Ault disclose the claim requirement that the client sends a control system command and the security context to access the control system in the server.

Therefore, nowhere does the cite Ault disclose the claim requirements of requesting with the client a security context for the client, returning with the server the security context to the client, and transmitting from the client the security context and a control system command to access the control system in the server, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context.

Further, the claims require that the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations. Nowhere does the cited Ault discuss the claim requirement that the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations, in combination with the claim requirements of requesting with the client a security context for the client, returning with the server the security context to the client, and transmitting from the client the security context

and a control system command to access the control system in the server, where the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context.

For the above reasons, claims 1, 9, and 17 are patentable over the cited Ault, because the cited Ault does not teach or disclose all the claim limitations.

Claims 2-8, 10-16, 18-24

The Examiner has also rejected pending claims 2-8, 10-16, 18-24 that depend on the pending independent claims 1, 9, and 17 respectively. Applicants submit that these claims are patentable over the cited art because they depend from claims 1, 9, 17 respectively which are patentable over the cited art for the reason discussed above, and because the combination of the limitations in the dependent claims 2-8, 10-16, 18-24 and the base and intervening claims from which they depend provide further grounds of distinction over the cited art

Claims 2, 10, 18

Claims 2, 10, and 18 depend from claims 1, 9 and 17 respectively and further require that requesting the security client comprises the client requesting the server to impersonate the client to obtain the security context, further comprising accessing, with the server impersonating the client, the security context to return to the client.

The claims require that the client requests the server to obtain the security context by impersonating the client and returning the security context to the client.

The cited Ault discusses the server impersonating the client to return a protected file to a client, where the protected file is a Web document. However, nowhere does the cited Ault disclose the claim requirement that the server impersonates the client for returning the security context to the client. The security context of the claim requirements is different from the protected file of the cited Ault.

For the above reasons, claims 2, 10, and 18 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 3, 11, and 19

Claims 3, 11, and 19 depend from claims 2, 10, and 18 respectively and further require that the Distributed Computing Environment (DCE) protocol is used to provide the client security context, wherein the client uses the sec_login_become_initiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context.

The claims require the client to use the sec_login_become_intiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context.

The cited Ault (col. 7, lines 54-58, 60-67; col. 8, lines 1-19) discusses how the server impersonates the client within the DCE protocol and further discusses login commands. Nowhere does the cited Ault disclose the claim requirement of the client using the sec_login_become_intiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context.

The Examiner mentions that in the cited Ault a credential file is returned to the session manager process in col. 6: lines 50-57. However, the session manager process (Ault: reference numeral 62 of FIG. 3) in not in the client. Therefore, the cited Ault does not teach or disclose returning the requested security context to the client but discusses how credentials are processed in the server.

For the above reasons, claims 3, 11, and 19 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 4, 12, and 20

Claims 4, 12, and 20 depend from claims 1, 9 and 17 respectively and further require converting, with the server, the security context transmitted through the client program to a pointer to credential information of the client;

determining from the credential information, with the server, whether the client is authorized to invoke the transmitted control system command; and

executing, with the server, the control system command transmitted by the client if the client is authorized to invoke the command.

The claims require converting the security context transmitted through the client program to a pointer to a credential information of the client. The cited Ault discusses whether the user identity of a thread corresponding to the client has any associated credential. If so, access is granted to the client. Nowhere does the cited Ault disclose the claim requirement of converting the security context transmitted through the client program to a pointer to a credential information of the client.

For the above reasons, claims 4, 12, and 20 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 6, 14, and 22

Claims 6, 14, and 22 depend from claims 1, 9 and 17 respectively and further require that the client requests the security context through a remote procedure call.

The cited Ault discusses a Web server component running on the server that provides various security and other function and also discusses how the server plug-in component on the server calls the session manager through a remote procedure call. Nowhere does the cited Ault disclose the claim requirement that the client requests the security context through a remote procedure call. The remote procedure call (col. 6: lines 42-45) discussed in the cited Ault is for the server plug-in component to call the session manager (Ault: reference numeral 62). The cited

Ault teaches away from the claims because in the cited Ault the remote procedure call is from the server to the session manager associated with the server, whereas the claims require making a remote procedure call from the client.

For the above reasons, claims 6, 14, and 22 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 8, 16, and 24

Claims 8, 16, and 24 depend from claims 7, 15, and 23 respectively and further require that the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

The cited Ault (col. 7, lines 44-49) discusses that the server returns the request file to the client to complete servicing of the original requests. A routine then continues with the server returning the user identity back to the session manager pool and the server making a remote procedure call to release the user. Nowhere does the cited Ault disclose the claim requirement that the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

For the above reasons, claims 8, 16, and 24 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-24 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 50-0585.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: January 22, 2004

By: Rabindranath Dutta

Rabindranath Dutta

Registration No. 51,010

Please direct all correspondences to:

David Victor

Konrad Raynes Victor & Mann, LLP

315 South Beverly Drive, Ste. 210

Beverly Hills, CA 90212

Tel: 310-553-7977

Fax: 310-556-7984